

Application No.: 09/434,440

Docket No.: 20162-00534-US

REMARKS

The Office Action and references cited have been carefully considered. The foregoing amendment to the claims are believed to overcome the rejections under 35 U.S.C. § 102(a).

The present invention is an improvement of the scheme disclosed in the cited Fujioka reference. The voting scheme according to the Fujioka reference is explained on pages 246-248, in which a vote v_i is encrypted by a key k_i to produce $x_i = q(v_i, k_i)$. The encryption function q is based on a bit-commitment scheme.

After checking the existence of the voter's x_i on a table, the voter has to send his key k_i to the counter.

In the present invention, each voter encrypts a vote with a counter's public key, the counter apparatus can decrypt the encrypted vote by using the counter's own secret key. Therefore, it is not necessary for the voters to send their keys to the counter. In addition, the counter apparatus is comprised of a plurality of distributed counter apparatuses and the secret key is split into plural partial secret keys and held separately by the plurality of distributed counter apparatuses so that any one of the distributed counter apparatuses cannot decrypt any encrypted vote by itself at arbitrary time.

The cited Herschberg reference relates to a secure electronic voting system. In general, since security of votes depends on the signature of the administrator, it is not possible to prevent fraudulent votes by the administrator himself. In the Herschberg system, each voter encrypts his one-time password with a public key, attaches the encrypted password to his vote and sends the vote and the encrypted password to a counter. There are provided plural examiners (or counters) each holding corresponding one of divided pieces of a secret key of the public encryption system, and the examiners cooperatively decrypt the encrypted

Application No.: 09/434,440

Docket No.: 20162-00534-US

password attached to each vote to check validity of the vote and also to check if the vote is attached with a correct signature of the administrator. The administrator does not know the voter's password and therefore cannot add fraudulent votes. Any number of the examiners less than the threshold singularly or cooperatively cannot decrypt the encrypted password, thus preventing fraudulent votes by a number of the examiners less than the threshold.

The Herschberg system differs from the present invention in that in the former, the threshold scheme is applied to only such authentication information as password, while in the latter, the threshold scheme is applied to the vote itself.

In view of the above, consideration and allowance are, therefore, respectfully solicited.

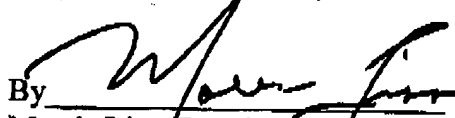
In the event the Examiner believes an interview might serve to advance the prosecution of this application in any way, the undersigned attorney is available at the telephone number noted below.

The Director is hereby authorized to charge any fees, or credit any overpayment, associated with this communication, including any extension fees, to CBLH Deposit Account No. 22-0185.

Dated:

2/10/04

Respectfully submitted,

By 

Morris Liss, Reg. No. 24,510
CONNOLLY BOVE LODGE & HUTZ LLP
1990 M Street, N.W., Suite 800
Washington, DC 20036-3425
(202) 331-7111
(202) 293-6229 (Fax)
Attorney for Applicant